UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, v. SUE MI TERRY, Defendant.	Case No. 24 Cr. 427 (LGS)

THE GOVERNMENT'S UNCLASSIFIED BRIEF IN OPPOSITION TO THE DEFENDANT'S MOTION TO DISCLOSE AND SUPPRESS FISA MATERIALS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

U.S. Constitution

Statutes

Other Authorities

I. INTRODUCTION

The Government submits this unclassified brief in opposition to Defendant Sue Mi Terry's (Terry) motion to suppress information obtained under the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1801, *et seq*., and to disclose FISA materials to the defense. (Dkt. 40, (Mem.)).[1] In relevant part, Terry requests that this Court "scrutinize the FISA applications and materials, suppress any evidence and fruits that were obtained unlawfully, and order disclosure of the FISA materials to the defense." (Mem. 46). Through her motion, Terry triggered this Court's review of the FISA application(s), order(s), and related materials (*i.e.*, the FISA materials)[2] related to the FISA-authorized electronic surveillance and physical search at issue in this case to determine whether the FISA information was lawfully acquired and whether the electronic surveillance and physical search conformed with an order of authorization or approval.[3]

FISA specifies:

> [W]henever a motion is made pursuant to subsection (e) . . . to discover or obtain applications or orders or other materials relating to electronic surveillance [or physical search] or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance [or physical search] under this Act, the United States district court . . . shall, . . . if the

---

[1] In its March 6, 2025 order this Court granted the Government's request for an adjustment of the briefing scheduling for the classified portion of the Government's opposition to Terry's pretrial motions, allowing the Government to file its classified brief by June 17, 2025. (Dkt. 49). The Government timely filed its unclassified opposition to Terry's pretrial motions, Dkt. 52, and has filed its classified brief pursuant to the Court's order. The pagination and footnote numbering in this unclassified brief differ from the classified brief due to redactions.

[2] **[CLASSIFIED INFORMATION REDACTED]**

[3] The FISA provisions that address electronic surveillance are found at 50 U.S.C. §§ 1801-1812; those that address physical search are found at 50 U.S.C. §§ 1821-1829. These two sets of provisions are in many respects parallel and almost identical. Citations herein are generally to the two sets of provisions in parallel, with the first citation being to the relevant electronic surveillance provision, and the second citation being to the relevant physical search provision.

> Attorney General[4] files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review *in camera* and *ex parte* the application, order, and such other materials relating to the surveillance [or search] as may be necessary to determine whether the surveillance [or search] of the aggrieved person was lawfully authorized and conducted.

50 U.S.C. §§ 1806(f), 1825(g). The Government is filing herewith such an affidavit.[5] Accordingly, this Court must conduct an *in camera, ex parte* review of the FISA materials relevant to Terry's motion consistent with 50 U.S.C. §§ 1806(f) and 1825(g).[6]

As discussed below, this Court's *in camera, ex parte* review will show that: (1) suppression of the FISA information is unwarranted because the electronic surveillance and physical search at issue were lawfully authorized and conducted in compliance with FISA; (2) disclosure of the FISA materials to Terry is not authorized because this Court can determine the legality of the FISA-authorized electronic surveillance and physical search without disclosing the FISA materials or portions thereof, and (3) due process does not otherwise require disclosure of the FISA applications to the defense.

A. BACKGROUND

[CLASSIFIED INFORMATION REDACTED]

On July 15, 2024, a grand jury in this district returned an indictment charging Terry with

---

[4] As defined in FISA, "Attorney General" means the Attorney General of the United States (or Acting Attorney General), the Deputy Attorney General, or, upon the designation of the Attorney General, the Assistant Attorney General for National Security (AAG/NS). *See* 50 U.S.C. §§ 1801(g), 1821(1). Attorney General Eric H. Holder, Jr., made such a designation on April 24, 2009.

[5] The Government is filing both publicly and as an exhibit in the Sealed Appendix the Declaration and Claim of Privilege, an affidavit executed by Attorney General Pamela Bondi. *See* Sealed Ex. 1.

[6] **[CLASSIFIED INFORMATION REDACTED]**

one count of conspiring to violate the Foreign Agents Registration Act (FARA), in violation of 18 U.S.C. § 371; and one count of failing to register under FARA, in violation of 22 U.S.C. §§ 612(a) and 618(a)(1), and 18 U.S.C. § 2. (Indictment (Ind.), Dkt. 2).

On July 22, 2024, pursuant to 50 U.S.C. §§ 1806(c) and 1825(d), the Government provided notice to this Court and Terry of its intent to offer into evidence or otherwise use or disclose information obtained or derived from electronic surveillance and physical search conducted pursuant to FISA. (Dkt. 11).

On February 26, 2025, Terry filed her motion seeking, among other relief, that this Court "scrutinize the FISA applications and materials, suppress any evidence and fruits that were obtained unlawfully, and order disclosure of the FISA materials to the defense." (Mem. 46).

[CLASSIFIED INFORMATION REDACTED]

B. OVERVIEW OF THE FISA AUTHORITIES AT ISSUE

[CLASSIFIED INFORMATION REDACTED]

1. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

2. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

3. The FISC's Findings

[CLASSIFIED INFORMATION REDACTED]

The various findings required under FISA to approve electronic surveillance or physical search, and the Government's submissions to the FISC addressing those requirements in the dockets at issue, are discussed in detail below.

II. THE FISA PROCESS

To aid this Court's review, this brief provides an overview of the FISA process. It covers the FISC's and the Attorney General's roles prescribed in FISA, the requirements to apply for a FISA order to conduct electronic surveillance or physical search, the findings the FISC must make in issuing such an order, and the procedures and standards governing a district court's review of FISA authorities when evidence obtained or derived therefrom is used in criminal proceedings. Not every part of FISA discussed below is at issue, and this brief notes where certain aspects of FISA are not directly implicated in this matter. This brief still discusses those other aspects to give context for this Court's review of the surveillance and search at issue.

A. OVERVIEW OF FISA

Enacted in 1978, and subsequently amended, FISA authorizes the Chief Justice of the United States to designate eleven United States district judges to sit as judges of the FISC. 50 U.S.C. § 1803(a)(1). The FISC judges are empowered to consider *ex parte* applications submitted by the Executive Branch for electronic surveillance and physical search when a significant purpose of the application is to obtain foreign intelligence information, as defined in FISA. Rulings of the FISC are subject to review by the Foreign Intelligence Surveillance Court of Review (FISC of Review), which is composed of three United States district or circuit judges who are designated by the Chief Justice. *Id.* § 1803(b).

FISA provides a statutory procedure whereby the Executive Branch may obtain a judicial order authorizing the use of electronic surveillance and/or physical search in the United States when a significant purpose is the collection of foreign intelligence information.[7] *Id.* §§ 1804(a)(6)(B), 1823(a)(6)(B). Under FISA, foreign intelligence information means:

---

[7] **[CLASSIFIED INFORMATION REDACTED]**

> (1) information that relates to, and if concerning a United States person[8] is necessary to, the ability of the United States to protect against—
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

50 U.S.C. § 1801(e); *see also id.* § 1821(1) (adopting the definitions from 50 U.S.C. § 1801). Except for emergency authorizations, FISA requires the Government to obtain a court order before it conducts any electronic surveillance or physical search.

FISA provides that the Attorney General may authorize the emergency employment of electronic surveillance and physical search if the Attorney General:

> (A) reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance [or physical search] to obtain foreign intelligence information before an order authorizing such surveillance [or physical search] can with due diligence be obtained;
>
> (B) reasonably determines that the factual basis for the issuance of an order under this title to approve such electronic surveillance [or physical search] exists;
>
> (C) informs, either personally or through a designee, a judge having jurisdiction under [50 U.S.C. § 1803] at the time of such authorization that the decision has been made to employ emergency electronic surveillance [or physical search]; and
>
> (D) makes an application in accordance with this title to a judge having jurisdiction under section 103 as soon as practicable, but not later than 7 days

[8] **[CLASSIFIED INFORMATION REDACTED]**

> after the Attorney General authorizes such electronic surveillance [or physical search].

50 U.S.C. §§ 1805(e)(1), 1824(e)(1).[9]

B. THE FISA APPLICATION

An application to conduct electronic surveillance pursuant to FISA must contain, among other things:

> (1) the identity of the federal officer making the application;
>
> (2) the identity, if known, or a description of the specific target of the electronic surveillance;
>
> (3) a statement of the facts and circumstances supporting probable cause to believe that the target is a foreign power or an agent of a foreign power, and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
>
> (4) a statement of the proposed minimization procedures;
>
> (5) a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;
>
> (6) a certification, discussed below, of a high-ranking official;
>
> (7) a summary of the manner or means by which the electronic surveillance will be effected and a statement whether physical entry is required to effect the electronic surveillance;
>
> (8) the facts concerning and the action taken on all previous FISA applications involving any of the persons, facilities, or places specified in the application; and
>
> (9) the proposed duration of the electronic surveillance.

50 U.S.C. § 1804(a)(1)-(9).

An application to conduct a physical search pursuant to FISA must contain similar information as an application to conduct electronic surveillance, except that an application to

---

[9] **[CLASSIFIED INFORMATION REDACTED]**

conduct a physical search must also contain a statement of the facts and circumstances justifying an applicant's belief that "the premises or property to be searched contains foreign intelligence information" and that each "premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from" the target. *Id.* § 1823(a)(1-8), (a)(3)(B), (C).

1. The Certification

An application to the FISC for a FISA order must include a certification from a high-ranking Executive Branch official with national security responsibilities that:

> (A) the certifying official deems the information sought to be foreign intelligence information;
>
> (B) a significant purpose of the surveillance is to obtain foreign intelligence information;
>
> (C) such information cannot reasonably be obtained by normal investigative techniques;
>
> (D) designates the type of foreign intelligence information being sought according to the categories described in [50 U.S.C. §] 1801(e); and
>
> (E) includes a statement of the basis for the certification that –
>
> > (i) the information sought is the type of foreign intelligence information designated; and
> >
> > (ii) such information cannot reasonably be obtained by normal investigative techniques.

50 U.S.C. § 1804(a)(6); *see also id.* § 1823(a)(6).

As originally enacted, FISA required that a high-ranking member of the Executive Branch of Government certify that "the purpose" of the FISA application was to obtain foreign intelligence information. In 2001, FISA was amended as part of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act

(USA PATRIOT Act).[10] The USA PATRIOT Act changed FISA so that a high-ranking official must now certify that the acquisition of foreign intelligence information is "a significant purpose" of the requested surveillance or search. *See id.* §§ 1804(a)(6)(B), 1823(a)(6)(B).

2. Minimization Procedures

The Attorney General has adopted, and the FISC has approved, minimization procedures that regulate the acquisition, retention, and dissemination of non-publicly available information concerning unconsenting U.S. persons that was obtained through FISA-authorized electronic surveillance or physical search, including persons who are not the targets of the FISA authorities. FISA requires that such minimization procedures be:

> reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

50 U.S.C. §§ 1801(h)(1), 1821(4)(A).

Minimization procedures also include "procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." *Id.* §§ 1801(h)(3), 1821(4)(c).

[CLASSIFIED INFORMATION REDACTED]

3. Attorney General's Approval

FISA also requires that the Attorney General approve applications for electronic surveillance and/or physical search before they are presented to the FISC, "based upon [a] finding that it satisfies the criteria and requirements" in FISA. *Id.* §§ 1804(a), 1823(a).

---

[10] Pub. L. No. 107-56, 115 Stat. 272 (2001).

C. THE FISC'S ORDERS

Once approved by the Attorney General, the application is submitted to the FISC and assigned to one of its judges. The FISC may approve the requested electronic surveillance and/or physical search only upon finding, among other things, that:

> (1) the application has been made by a Federal officer and has been approved by the Attorney General;
>
> (2) there is probable cause to believe that (A) the target of the electronic surveillance and/or physical search is a foreign power or an agent of a foreign power, and that (B) the facilities or places at which the electronic surveillance is directed are being used, or are about to be used, by a foreign power or an agent of a foreign power, or that the premises or property to be searched is, or is about to be, owned, used, possessed by, or is in transit to or from, a foreign power or an agent of a foreign power;
>
> (3) the proposed minimization procedures meet the statutory requirements set forth in section 1801(h) (electronic surveillance) and section 1821(4) (physical search);
>
> (4) the application contains all of the statements and certifications required by section 1804 (electronic surveillance) or section 1823 (physical search); and
>
> (5) if the target is a United States person, the certifications are not clearly erroneous.

50 U.S.C. §§ 1805(a)(1)-(4), 1824(a)(1)-(4).

FISA defines "foreign power" to mean—

> (1) a foreign government or any component, thereof, whether or not recognized by the United States;
>
> (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
>
> (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
>
> (4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of United States persons;

(6) an entity that is directed and controlled by a foreign government or governments; or

(7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

50 U.S.C. § 1801(a)(1)-(7); *see also id.* § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

"Agent of a foreign power" means—

(1) any person other than a United States person, who—

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4), irrespective of whether the person is inside the United States;

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances indicate that such person may engage in such activities, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;

(C) engages in international terrorism or activities in preparation therefore [sic];

(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign power, or knowingly aids or abets any person in the conduct of such proliferation or activities in preparation therefor, or knowingly conspires with any person to engage in such proliferation or activities in preparation therefor; or

(2) any person who—

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which

> activities involve or are about to involve a violation of the criminal statutes of the United States;
>
> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
>
> (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
>
> (E) knowingly aids or abets any person in the conduct of activities described in subparagraphs (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraphs (A), (B), or (C).

50 U.S.C. § 1801(b)(1), (2); *see also id.* § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

FISA specifies that no U.S. person may be considered a foreign power or an agent of a foreign power based solely on First Amendment protected activities. *Id.* §§ 1805(a)(2)(A), 1824(a)(2)(A). Although First Amendment protected activities cannot form the sole basis for FISA-authorized electronic surveillance or physical search, the FISC may consider them if other activity indicates the target is an agent of a foreign power. *United States v. Rosen*, 447 F. Supp. 2d 538, 548-49 (E.D. Va. 2006); *United States v. Rahman*, 861 F. Supp. 247, 252 (S.D.N.Y. 1994), *aff'd*, 189 F.3d 88 (2d Cir. 1999).

The FISA application must establish probable cause to believe the target is acting as an agent of a foreign power at the time of the application. *United States v. Squillacote*, 221 F.3d 542, 554 (4th Cir. 2000). However, in determining whether probable cause exists, FISA allows a judge to "consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." 50 U.S.C. §§ 1805(b), 1824(b).

If the FISC makes all necessary findings and concludes the FISA application meets the statutory provisions, the FISC issues an *ex parte* order authorizing the electronic surveillance

and/or physical search requested in the application. 50 U.S.C. §§ 1805(a), 1824(a). The order must:

> (1) . . . specify—
>
> > (A) the identity, if known, or a description of the specific target of the [collection];
> >
> > (B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known [and/or of each of the premises or properties to be searched];
> >
> > (C) the type of information sought to be acquired and the type of communications or activities to be subjected to the [electronic] surveillance [and/or the type of information, material, or property to be seized, altered, or reproduced through the physical search];
> >
> > (D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance [and/or a statement of the manner in which the physical search will be conducted and, whenever more than one physical search is authorized under the order, the authorized scope of each search and what minimization procedures shall apply to the information acquired by each search]; and
> >
> > (E) the period of time during which the electronic surveillance is approved [and/or the period of time during which physical searches are approved; and]
>
> (2) . . . direct—
>
> > (A) that the minimization procedures be followed . . . .

Id. §§ 1805(c)(1), (2)(A), 1824(c)(1), (2)(A).

Initial FISC approval for electronic surveillance and/or physical search targeting a U.S. person may be approved for up to 90 days, and those targeting a non-U.S. person may be approved for up to 120 days. *Id.* §§ 1805(d)(1), 1824(d)(1). The FISC may renew such approval, but only if the Government submits another application that complies with FISA's requirements. A renewal for electronic surveillance or physical search targeting a U.S. person

may be approved for up to 90 days, and one targeting a non-U.S. person may be approved for up to one year.[11] *See* 50 U.S.C. §§ 1805(d)(2), 1824(d)(2).

III. THE DISTRICT COURT'S REVIEW OF FISC ORDERS

FISA authorizes the use of information obtained or derived from electronic surveillance and physical search in a criminal prosecution, provided that advance authorization is obtained from the Attorney General, *see* 50 U.S.C. §§ 1806(b), 1825(c), and that notice of the surveillance and search is given to the court and to each aggrieved person against whom the information is to be used. *Id.* §§ 1806(c)–(d), 1825(d)–(e).[12] Upon receiving notice, the aggrieved person against whom FISA information is to be used may move to suppress the information on two grounds: (1) that "the information was unlawfully acquired"; or (2) that "the surveillance [or search] was not made in conformity with an order of authorization or approval." *Id.* §§ 1806(e), 1825(f).

In addition, FISA provides that a defendant who is an aggrieved person may file "a motion or request . . . pursuant to any other statute or rule of the United States . . . to discover or obtain applications or orders or other materials relating to electronic surveillance [or physical search] or to discover, obtain, or suppress evidence or information obtained or derived [therefrom]." 50 U.S.C. §§ 1806(f), 1825(g). In adjudicating such a "motion or request," if the district court "determines that the surveillance [or search] was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived [therefrom] or otherwise grant the motion of the aggrieved

---

[11] The FISC retains the authority to review, before the end of the authorized period of electronic surveillance or physical search, the Government's compliance with the requisite minimization procedures. *See* 50 U.S.C. §§ 1805(d)(3), 1824(d)(3).

[12] Terry is an "aggrieved person" under FISA, and as noted above, was provided with notice of her status as such and of the Government's intent to use FISA-obtained or -derived information against her in this case.

person." *Id.* §§ 1806(g), 1825(h). "If the court determines that the surveillance [or search] was lawfully authorized and conducted," however, "it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure." *Id.*

A. THE DISTRICT COURT'S REVIEW IS TO BE CONDUCTED *IN CAMERA* AND *EX PARTE*

Once an aggrieved person has moved for disclosure of FISA materials or suppression of FISA information, "if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States," the district court adjudicating the motion "shall, notwithstanding any other law," "review in camera and ex parte the application, order, and such other materials relating to the surveillance [or search] as may be necessary to determine whether the surveillance [or search] of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. §§ 1806(f), 1825(g).

[CLASSIFIED INFORMATION REDACTED]

In conducting its *in camera*, *ex parte* review, the district court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance *only where such disclosure is necessary to make an accurate determination of the legality of the surveillance* [*or search*]." 50 U.S.C. §§ 1806(f), 1825(g) (emphasis added). The district court's discretion to disclose FISA materials to an aggrieved defendant is thus highly circumscribed, and its exercise is unwarranted unless the court first concludes that it is unable to accurately determine the legality of the FISA authorities even after reviewing the Government's *in camera* and *ex parte* submissions. *See, e.g.*, *Abu-Jihaad*, 531 F. Supp. 2d at 299, 311 (D. Conn. 2008) ("The Court has read and re-read each [Government] submission and [FISC] order. Having done so, the Court is satisfied that disclosure and an adversary hearing are not required in this case. The Court is able to

[determine] the legality of the surveillance on the basis of the materials submitted . . . *ex parte* and *in camera*."); *see also United States v. Abu-Jihaad*, 630 F.3d 102, 129 (2d Cir. 2010) (affirming based on an independent review of the materials submitted to the district court). As the court stated in *United States v. Daoud*, "[u]nless and until a district judge performs his or her statutory duty of attempting to determine the legality of the surveillance without revealing any of the fruits of the surveillance to defense counsel, there is no basis for concluding that disclosure is necessary in order to avert an erroneous conviction." 755 F.3d 479, 484 (7th Cir. 2014).

1. *In Camera, Ex Parte* Review is the Rule

With respect to FISA's *in camera*, *ex parte* review procedures, courts have "emphasized that 'disclosure and an adversary hearing are the exception occurring *only* when necessary.'" *United States v. Omar*, 786 F.3d 1104, 1110 (8th Cir. 2015) (emphasis in original) (quoting *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982)). The Second Circuit has similarly explained that "disclosure of FISA materials is the exception and *ex parte*, *in camera* determination is the rule." *Abu-Jihaad*, 630 F.3d at 129 (internal quotation marks and citation omitted); *accord United States v. Stewart*, 590 F.3d 93, 128 (2d Cir. 2009); *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984), *superseded by statute on other grounds*, USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001), *as recognized in Abu-Jihaad*, 630 F.3d at 119.[13] Terry does not dispute that *ex parte, in camera* review is the rule, conceding in her motion "that 'disclosure of the FISA materials [to the defense] is the exception and *ex parte*, *in*

[13] *Duggan* allowed that disclosure could be warranted in narrow circumstances, including "if the judge's initial review [of the government's submission] revealed potential irregularities such as 'possible misrepresentation of fact, vague identification of the persons to be surveilled[,] or surveillance records which include[] a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order.'" 743 F.2d at 78 (quoting S. Rep. No. 95-604, at 58 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3960).

camera determination is the rule.' *Abu Jihaad*, 630 F.3d at 129." (Mem. 50).

With one exception, every district court to have ruled on a motion to disclose FISA materials or to suppress FISA information has determined that it was able to adjudicate the legality of the FISA collection at issue based on its *in camera*, *ex parte* review,[14] and every appellate court to have reviewed such a determination has affirmed.[15] The one district court to have ordered disclosure of FISA materials to the defense was reversed on appeal. *See Daoud*, 755 F.3d at 484–85; *see also* 50 U.S.C. §§ 1806(h), 1825(i) (providing for interlocutory appellate review of orders granting motions to suppress FISA information or disclose FISA materials).

The materials in the Sealed Appendix confirm that there is no reason to depart from the "rule" of *ex parte, in camera* review here. This Court's review of these materials will demonstrate the FISC's proper justification for approving the authorities at issue and the Government's good-faith implementation of those authorities. This Court's review will further show the absence of any impropriety that could justify an adversarial hearing or disclosure of

---

[14] *See, e.g.*, *Abu-Jihaad*, 531 F. Supp. 2d at 310-11; *United States v. Al-Safoo*, 18-CR-696, 2021 WL 1750313, at *3–4 (N.D. Ill. May 4, 2021); *United States v. Kokayi*, 1:180cr-410 (LMB), 2019 WL 1186846, at *5–6 (E.D. Va. Mar. 13, 2019); *United States v. Chi Ping Ho*, 17 Cr. 779 (LAP), 2018 WL 5777025, at *5 (S.D.N.Y. Nov. 2, 2018); *United States v. Alimehmeti*, Case No. 16-398, Order Denying Motion to Suppress (Dkt. No. 67) (S.D.N.Y. Sept. 22, 2017); *United States v. Medunjanin*, No. 10 CR 19 1 (RJD), 2012 WL 526428, at *9 (E.D.N.Y. Feb. 16, 2012); *United States v. Warsame*, 547 F. Supp. 2d 982, 987 (D. Minn. 2008); *United States v. Benkahla*, 437 F. Supp. 2d 541, 554 (E.D. Va. May 17, 2006); *Rosen*, 447 F. Supp. 2d at 546; *United States v. Sattar*, No. 02 CR. 395 JGK, 2003 WL 22137012, at *6 (S.D.N.Y. Sept. 15, 2003); *United States v. Nicholson*, 955 F. Supp. 588, 592 & n.11 (E.D. Va. 1997); *United States v. Thomson*, 752 F. Supp. 75, 79 (W.D.N.Y. 1990); *United States v. Falvey*, 540 F. Supp. 1306, 1315-16 (E.D.N.Y. 1982).

[15] *See, e.g.*, *United States v. Turner*, 840 F.3d 336, 340 (7th Cir. 2016); *Omar*, 786 F.3d at 1110; *United States v. El-Mezain*, 664 F.3d 467, 565 (5th Cir. 2011); *United States v. Duka*, 671 F.3d 329, 338 (3d Cir. 2011); *United States v. Damrah*, 412 F.3d 618, 624 (6th Cir. 2005); *United States v. Isa*, 923 F.2d 1300, 1306 (8th Cir. 1991)); *United States v. Hamide*, 914 F.2d 1147, 1152-53 (9th Cir. 1990). *United States v. Ott*, 827 F.2d 473, 475-76 (9th Cir. 1987); *United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir. 1987); *Belfield*, 692 F.2d at 147.

FISA materials to the defense. Moreover, as with the Government's previous submissions to district courts concerning FISC-approved authorities, the FISA materials here were prepared and organized to facilitate straightforward judicial review. *See, e.g.*, *In re Kevork*, 634 F. Supp. 1002, 1008 (C.D. Cal. 1985) (upholding surveillance and observing that FISA materials under review were "straightforward and readily understood"), *aff'd*, 788 F.2d 566 (9th Cir. 1986). On their face, the materials allow for an accurate judicial determination of whether the electronic surveillance and physical search at issue were lawfully authorized and conducted. Indeed, as is typical in cases involving electronic surveillance and physical search conducted pursuant to FISA, "the determination of legality in this case is not complex." *Belfield*, 692 F.2d at 147; *see also Abu-Jihaad*, 531 F. Supp. 2d at 310 (similar); *Warsame*, 547 F. Supp. 2d at 987 (finding that the "issues presented by the FISA applications are straightforward and uncontroversial"). Consistent with the approach taken by many other courts, this Court can review the FISA materials *in camera* and *ex parte* and make the requisite legal determinations without the need for an adversary hearing or disclosure of classified materials to the defense.

Apart from the specific harms that would result from disclosing the FISA materials in this case, as detailed in the classified declaration of a high-ranking FBI official in support of the Declaration and Claim of Privilege of Attorney General Bondi, the underlying rationale for non-disclosure is clear. "Congress has a legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated to *anyone* not involved in [a] surveillance operation." *Ott*, 827 F.2d at 477 (emphasis in original); *accord Medunjanin*, 2012 WL 526428, at *9 (finding that "unsealing the FISA materials . . . would provide the defense with unnecessary details of an extraordinarily sensitive anti-terrorism investigation"). In particular, the importance of protecting sensitive

intelligence sources cannot be overstated. If such sources believe that the United States "will be unable to maintain the confidentiality of its relationship to them, many [of those sources] could well refuse to supply information." *CIA v. Sims*, 471 U.S. 159, 175 (1985).

When considering whether the disclosure of classified sources, methods, techniques, or other information would harm the national security, courts have generally refrained from superseding the judgments of Executive Branch officials responsible for determining whether a particular disclosure would present an unacceptable risk of compromising intelligence-gathering processes. Among other issues, such judgments include consideration of whether certain information, which may not appear sensitive on its own, could be pieced together with a mosaic of other information (both public and non-public) to permit adversaries to glean insights enabling them to defeat U.S. counterintelligence efforts. *See, e.g.*, *Sims*, 471 U.S. at 179–80 ("The Director reasonably concluded that an observer who is knowledgeable about a particular intelligence research project . . . could, upon learning that research was performed at a certain institution, . . . deduce the identities of the individual researchers who are protected 'intelligence sources.'"); *United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989) ("Things that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods."). That consideration further underscores how disclosing FISA materials or conducting an adversary hearing is not only unnecessary to adjudicate Terry's Motion, but could also result in heightened risks to national security that courts have consistently sought to avoid.

Indeed, Congress enacted FISA's *in camera*, *ex parte* review procedures to account for such risks in accommodating the judiciary's need to review any FISA authorities that may be

implicated in litigation against aggrieved persons. As the D.C. Circuit explained in *Belfield*:

> Congress recognized the need for the Executive to engage in and employ the fruits of clandestine surveillance without being constantly hamstrung by disclosure requirements. The statute is meant to reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights. In FISA the privacy rights of individuals are ensured not through mandatory disclosure, but through its provisions for in-depth oversight of FISA surveillance by all three branches of government and by a statutory scheme that to a large degree centers on an expanded conception of minimization that differs from that which governs law-enforcement surveillance.

692 F.2d at 148 (internal quotation marks and citations omitted); *accord Daoud*, 755 F.3d at 483 ("[FISA] is an attempt to strike a balance between the interest in full openness of legal proceedings and the interest in national security, which requires a degree of secrecy concerning the government's efforts to protect the nation.").

2. *In Camera, Ex Parte* Review Is Constitutional

Since FISA's enactment, litigants have challenged the constitutionality of its *in camera, ex parte* review procedures on various grounds. For example, the defendants in *United States v. Dhirane* "argue[d] that it was contrary to our constitutionally established adversary system to deny their counsel, who possessed the requisite security clearance, access to the [FISA] applications and supporting materials," and that FISA's procedures prevented them from vindicating their right to a *Franks* hearing. *See* 896 F.3d 295, 299 (4th Cir. 2018); *see also Franks v. Delaware*, 438 U.S. 154 (1978) (recognizing the right to an adversarial hearing on the validity of a warrant upon a preliminary showing of an intentional or reckless falsehood in the warrant affidavit). In rejecting these arguments, the court explained:

> The government notes that every federal court to have considered the constitutionality of these procedures has concluded that FISA reached a reasonable and therefore constitutional balance of competing interests. [collecting cases] And we share that view. It is consistent with the general notion, even in the criminal context, that the right to an adversarial proceeding to determine disputes of fact is not absolute.

Dhirane, 896 F.3d at 300 (citing in part *Kaley v. United States*, 571 U.S. 320, 338 (2014), and *Taglianetti v. United States*, 394 U.S. 316, 317 (1969)). Like those other courts, the Second Circuit has repeatedly upheld the constitutionality of FISA's *in camera*, *ex parte* review provisions. *See Stewart*, 590 F.3d at 126 (concluding that "the procedures fashioned in FISA [are] a constitutionally adequate balancing of the individual's Fourth Amendment rights against the nation's need to obtain foreign intelligence information" (quoting *Duggan*, 743 F.2d at 73)); *Abu-Jihaad*, 630 F.3d at 117.

In sum, because Attorney General Bondi stated under oath that disclosing or conducting an adversary hearing with respect to the FISA materials would harm national security, Terry's Motion must be adjudicated using FISA's review procedures. Those procedures are constitutional and impose a general "rule" of *in camera*, *ex parte* review. There is no basis to depart from that rule in this case, and this Court should accordingly review the FISA materials *in camera* and *ex parte* when determining whether the electronic surveillance and physical search at issue were "lawfully authorized and conducted." 50 U.S.C. §§ 1806(g), 1825(h).

Finally, the Government notes that Terry specifically requests that this Court perform an *in camera*, *ex parte* review of the FISA materials: "Thus, Dr. Terry respectfully requests that the Court review such materials *in camera* and *ex parte*….". (Mem. 48). The Government has prepared and submits the instant brief and related materials for this purpose.

B. THE DISTRICT COURT'S SUBSTANTIVE REVIEW

An application to conduct electronic surveillance or physical search under FISA is "subject to 'minimal scrutiny by the courts,' both upon initial presentation [to the FISC] and subsequent challenge [before a district court]." *Abu-Jihaad*, 630 F.3d at 130 (quoting *Duggan*, 743 F.2d at 77). "[A]bsent a showing sufficient to trigger a *Franks* hearing," "'the

representations and certifications submitted in support of an application for FISA surveillance should be presumed valid' by a reviewing court." *Id.* (quoting *Duggan*, 743 F.2d at 77 n.6). "Of course, even minimal scrutiny is not toothless." *Id.* In assessing whether evidence was lawfully collected from FISC-approved surveillance or search, "a reviewing district court must consider: (1) whether the certification by the Executive Branch in support of the FISA application was properly made; (2) whether the application established probable cause; and (3) whether the collection followed proper minimization procedures." *United States v. Liu*, 19-CR-804 (VEC) 2021 WL 6127396, at *1 (S.D.N.Y. Dec. 28, 2021) (citing *Abu-Jihaad*, 630 F.3d at 130–31); *see also Chi Ping Ho*, 2018 WL 5777025, at *5 (articulating same three-part test). The discussion immediately below addresses the standards of review applicable to this Court's assessment of the FISC's probable cause findings and the Executive Branch certification(s) at issue. The standards governing this Court's assessment of compliance with proper minimization procedures are addressed in Section IV.C of this memorandum.

1. Standard of Review of Probable Cause

Courts have not definitively resolved whether the FISC's probable cause findings should be reviewed *de novo* or deferentially.[16] In the Second Circuit, district courts "tend to give the FISC's [probable cause] determination due deference." *Liu*, 2021 WL 6127396, at *1; *see also Abu-Jihaad*, 630 F.3d at 130 (observing that the "standard of judicial review applicable to FISA warrants is deferential," although "the government's detailed and complete submissions . . . would easily allow it to clear a higher standard of review"); *United States v. Fishenko*, No. 12

[16] *Compare, e.g.*, *Turner*, 840 F.3d at 340 (applying *de novo* review), *with United States v. Ahmed*, No. 1:06-CR-147-WSD-GGB, 2009 U.S. Dist. Lexis 120007, at *21 (N.D. Ga. Mar. 19, 2009) (concluding that the FISC's "determination of probable cause should be given 'great deference' by the reviewing court").

CV 626 (SJ), 2014 WL 4804215, at *3–5 (E.D.N.Y. Sept. 25, 2014) (similar); *Medunjanin*, 2012 WL 526428, at *6-7 (affording deferential review, while observing this "does not mean that such review is superficial"). In any event, the FISA materials here demonstrate that the FISC's probable cause determinations readily satisfy even a *de novo* standard of review.

2. Probable Cause Standard Under FISA

For the FISC to approve electronic surveillance or physical search, FISA requires a finding of probable cause that the target is a foreign power or an agent of a foreign power, and that each facility or place at which the surveillance is directed is being used, or is about to be used, by a foreign power or an agent thereof (or, for physical search, that the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from, a foreign power or an agent thereof). 50 U.S.C. §§ 1805(a), 1824(a). It is this standard—not the standard applicable to a criminal search warrant—that this Court must apply. *See Abu-Jihaad*, 630 F.3d at 130–31; *see also Omar*, 786 F.3d at 1111 ("[R]ather than focusing on probable cause to believe that a person has committed a crime, the FISA standard focuses on the status of the target as a foreign power or an agent of a foreign power." (quoting *El-Mezain*, 664 F.3d at 564)).

[CLASSIFIED INFORMATION REDACTED]

The Second Circuit has repeatedly affirmed the constitutionality of FISA's probable cause requirements under the Fourth Amendment, both before and after the USA PATRIOT Act modified FISA in 2001, confirming that obtaining foreign-intelligence information need only be "a significant purpose" (as opposed to *the primary* purpose) of the electronic surveillance or physical search. *See Abu-Jihaad*, 630 F.3d at 120.[17] *Abu-Jihaad*'s analysis of this issue relied to

[17] Numerous other courts have also affirmed the constitutionality of FISA's probable cause requirements. *See Abu-Jihaad*, 630 F.3d at 120 (collecting more than a dozen cases). The one decision holding otherwise—*i.e.*, that FISA's probable cause standard, in light of the USA

a significant extent on the Supreme Court's decision in *United States v. U.S. District Court (Keith)*, 407 U.S. 297 (1972). There, in considering the Fourth Amendment's warrant requirement and the standards for conducting traditional law enforcement wiretapping under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (hereinafter, "Title III"), the Court indicated that the Fourth Amendment would countenance different standards for a warrant to conduct domestic security surveillance. *See id.* at 321–22. With particular relevance here, *Keith* reasoned (1) that "the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency"; (2) that the "focus of . . . surveillance [in domestic security investigations] may be less precise than that directed against more conventional types of crime"; (3) that unlike ordinary criminal investigations, "[t]he gathering of security intelligence is often long range and involves the interrelation of various sources and types of information"; and (4) that the "exact targets of such surveillance may be more difficult to identify" than in surveillance targeting ordinary criminals. *Id.* *Keith* was decided before FISA's enactment and only addressed *domestic* security surveillance. *See id.* at 321–22 (expressly reserving judgment on the issue of warrantless surveillance directed at the "activities of foreign powers or their agents"). However, as the Second Circuit has recognized, *Keith*'s rationale applies *a fortiori* to foreign intelligence surveillance, where the Government's interests would generally be even more compelling. *See Abu-Jihaad*, 630 F.3d at 122 (observing that *Keith*'s considerations "supporting different warrant standards [for domestic intelligence] pertain equally to foreign intelligence surveillance.").[18]

PATRIOT Act's "significant purpose" modification, violates the Fourth Amendment—was vacated on standing grounds. *Mayfield v. United States*, 504 F. Supp. 2d 1023 (D. Or. 2007), *vacated*, 599 F.3d 964, 973 (9th Cir. 2010).

[18] FISA's procedures were enacted partly in response to *Keith*, and numerous courts have recognized that those procedures satisfy the Fourth Amendment's requirement of reasonableness,

3. Standard of Review for Executive Branch Certifications

The certification that FISA requires for an application to conduct electronic surveillance or physical search is "subject to only minimal scrutiny by the courts" and "presumed valid." *Duggan*, 743 F.2d at 77 & n.6. In particular, "[t]he FISA Judge, in reviewing the application, is not to second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information." *Id.* When an aggrieved person challenges FISC-approved surveillance or search before the district court, the "reviewing court is to have no greater authority to second-guess the executive branch's certifications than has the FISA Judge." *Id.*; *see also Chi Ping Ho*, 2018 WL 5777025, at *5 (same).

For a FISA application targeting a non-United States person, "[t]he FISA Judge need only determine that the application contains all of the statements and certifications required by [FISA]." *Duggan*, 743 F.2d at 75. When a United States person is targeted, the FISC must also find that the certifications are "not clearly erroneous." *Id.* (citing 50 U.S.C. § 1805(a)). A "clearly erroneous" finding is established only when, "although there is evidence to support it, the reviewing court on the entire evidence is left with the definite and firm conviction that a mistake has been committed." *United States v. Islamic American Relief Agency*, No. 07-0087-CR-W-NKL, 2009 WL 5169536, at *4 (W.D. Mo. Dec. 21, 2009) (assessing certifications for applications targeting United States persons) (quoting *United States v. U.S. Gypsum Co.*, 333 U.S. 364, 395 (1948)).[19]

---

in view of the reasoning from *Keith* discussed above. *See, e.g.*, *Duggan*, 743 F.2d at 74; *In re Sealed Case*, 310 F.3d at 738, 746; *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987); *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987).

[19] **[CLASSIFIED INFORMATION REDACTED]**

4. FISA is Subject to the "Good-Faith" Exception

Even if a district court were to determine that a particular application to the FISC failed to satisfy FISA's requirements, any evidence obtained or derived from FISC-approved electronic surveillance or physical search would nonetheless be admissible under the "good faith" exception to the exclusionary rule, recognized in *United States v. Leon*, 468 U.S. 897 (1984). Courts have found that *Leon*'s good-faith exception would apply to FISA-acquired evidence. *See, e.g.*, *United States v. Ning Wen*, 477 F.3d 896, 898 (7th Cir. 2007); *Ahmed*, 2009 U.S. Dist. Lexis 120007, at *25 n.8. Moreover, there is no indication here that the FISC failed to act in a neutral and detached manner, or that any assertion in a FISA application was deliberately or recklessly false, as might warrant exclusion of evidence obtained pursuant to a FISC order of approval. *See Leon*, 468 U.S. at 926. To the contrary, this Court's review of the FISA materials will confirm that the officials who applied for and implemented the FISA authorities at issue did so in good faith, and that the Government reasonably relied on the FISC's order(s) of approval in conducting electronic surveillance and physical search. Thus, even if the Court questions whether sufficient probable cause supported a FISC order, the information obtained pursuant to that order would be admissible under *Leon*'s good faith exception.

Lastly, consistent with its underlying rationale, a court should not impose the exclusionary rule to punish an officer who acts in objectively reasonable reliance on a duly-issued warrant or enacted statute. In *Illinois v. Krull*, 480 U.S. 340 (1987), the Supreme Court "ruled categorically that 'suppressing evidence obtained by an officer acting in objectively reasonable reliance on a statute' would not further the purposes of the exclusionary rule, even if that statute is later declared unconstitutional." *Duka*, 671 F.3d at 346 (quoting *Krull*, 480 U.S. at 349-50. The same is true for warrants that are later determined to be invalid. *See United States*

v. Helton, 35 F.4th 511, 521 (6th Cir. 2022) (quoting *Leon* for the proposition "that if 'the evidence was obtained in objectively reasonable reliance on the subsequently invalidated search warrant, however, it should not be suppressed"). "Because the rule 'is designed to deter police misconduct,' it applies only where it will 'alter the behavior of individual law enforcement officers or the policies of their departments.'" *Duka*, 671 F.3d at 346 (quoting *Leon*, 468 U.S. at 916-18). Here, the exclusion of FISA information would serve no such deterrent purpose. *See Davis v. United States*, 564 U.S. 229, 237 (2011); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 282-84 (S.D.N.Y. 2000).

IV. THE ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH AT ISSUE WERE LAWFULLY AUTHORIZED AND CONDUCTED

This section, in Parts A and B, first discusses the materials in the Sealed Appendix to demonstrate, in light of the standards of review described above, that the FISA authorities in this matter were lawfully *authorized*. In Part C, this section then addresses the Government's good-faith compliance with proper minimization procedures and related requirements to demonstrate that the electronic surveillance and physical search at issue were lawfully *conducted*.

A. THE INSTANT FISA APPLICATION(S) SATISFIED FISA'S PROBABLE CAUSE STANDARDS

[CLASSIFIED INFORMATION REDACTED]

1. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

2. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

3. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

4. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

B. THE CERTIFICATION(S) COMPLIED WITH FISA

[CLASSIFIED INFORMATION REDACTED]

1. Foreign Intelligence Information

[CLASSIFIED INFORMATION REDACTED]

2. "A Significant Purpose"

[CLASSIFIED INFORMATION REDACTED]

3. Information Not Reasonably Obtainable Through Normal Investigative Techniques

[CLASSIFIED INFORMATION REDACTED]

C. THE ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH WERE CONDUCTED IN CONFORMITY WITH AN ORDER OF AUTHORIZATION OR APPROVAL

[CLASSIFIED INFORMATION REDACTED]

1. The Standard Minimization Procedures

[CLASSIFIED INFORMATION REDACTED]

FISA's legislative history and applicable case law demonstrate that the definitions of "minimization procedures" and "foreign intelligence information" were intended to take into account the realities of collecting foreign intelligence, including that the activities of those engaged in clandestine intelligence gathering or international terrorism are often not obvious on their face. *See Rahman*, 861 F. Supp. at 252–53. The degree to which information is required to be minimized may vary given the specifics of a particular investigation, such that less minimization at acquisition is justified when "the investigation is focusing on what is thought to be a widespread conspiracy" and more extensive surveillance is necessary "to determine the precise scope of the enterprise." *In re Sealed Case*, 310 F.3d at 741; *see also Bin Laden*, 126 F.

Supp. 2d at 286 (agreeing with the government that "more extensive monitoring and greater leeway in minimization efforts are permitted in a case like this given the world-wide, covert and diffuse nature of the international terrorist group(s) targeted"). Furthermore, the activities of foreign powers and their agents are often not obvious from an initial or cursory overhear of conversations. To the contrary, agents of foreign powers frequently engage in coded communications, compartmentalized operations, the use of false identities, and other practices designed to conceal the breadth and aim of their operations, organization, activities and plans. *See, e.g., United States v. Salameh*, 152 F.3d 88, 154 (2d Cir. 1998) (noting that two conspirators involved in the 1993 bombing of the World Trade Center in New York referred to the bomb plot as the "study" and to terrorist materials as "university papers"). As one court explained, "[i]nnocuous-sounding conversations may in fact be signals of important activity; information on its face innocent when analyzed or considered with other information may become critical." *In re Kevork*, 634 F. Supp. at 1017 (quoting H.R. Rep. No. 95-1283, pt. 1, at 55 (1978)); *see also In re Sealed Case*, 310 F.3d at 740–41 (comparing minimization under FISA and Title III); *Thomson*, 752 F. Supp. at 81 (noting that it is permissible to retain and disseminate "bits and pieces" of information until the information's "full significance becomes apparent") (citing H.R. Rep. No. 95-1283, pt. 1, at 58).

Likewise, "individual items of information, not apparently significant when taken in isolation, may become highly significant when considered together over time." *Rahman*, 861 F. Supp. at 252–53 (citing H.R. Rep. No. 95-1283, pt. 1, at 55, 59). In addition, the government may require greater flexibility in the FISA context due to the likelihood that some communications involving foreign agents will be carried out in a foreign language (as happened here). *See, e.g.*, *United States v. Mubayyid*, 521 F. Supp. 2d 125, 134 (D. Mass. 2007)

(upholding ten-year period for retention of FISA-acquired communications, including because the communications were in a foreign language). Basically, "courts have construed 'foreign intelligence information' broadly and sensibly allowed the government some latitude in its determination of what is foreign intelligence information." *Rosen*, 447 F. Supp. 2d at 551.

The nature of the foreign intelligence information sought also impacts implementation of the minimization procedures at the retention and dissemination stages. There is a legitimate need to conduct a thorough post-acquisition review of FISA information that involves a United States person who is acting as an agent of a foreign power. As Congress explained:

> It is "necessary" to identify anyone working with him in this network, feeding him information, or to whom he reports. Therefore, it is necessary to acquire, retain and disseminate information concerning all his contacts and acquaintances and his movements. Among his contacts and acquaintances, however, there are likely to be a large number of innocent persons. Yet, information concerning these persons must be retained at least until it is determined that they are not involved in the clandestine intelligence activities and may have to be disseminated in order to determine their innocence.

H.R. Rep. No. 95-1283, pt. 1, at 58. Indeed, as one court cautioned, when a United States person communicates with an agent of a foreign power, the government would be "remiss in meeting its foreign counterintelligence responsibilities" if it did not thoroughly "investigate such contacts and gather information to determine the nature of those activities." *Thomson*, 752 F. Supp. at 82. In light of these realities, Congress recognized that "no electronic surveillance can be so conducted that innocent conversations can be totally eliminated." *See* S. Rep. No. 95-701, at 39 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4008.

Accordingly, in reviewing the adequacy of minimization efforts, the test to be applied is neither whether innocent conversations were intercepted, nor whether mistakes were made with respect to particular communications. To the contrary, courts have emphasized the statement in FISA's legislative history that "[a]bsent a charge that the minimization procedures have been

disregarded completely, the test of compliance is whether a good faith effort to minimize was attempted." *Mubayyid*, 521 F. Supp. 2d at 135 (quoting S. Rep. No. 95-701, at 39–40 (1978)); *see also Scott v. United States*, 436 U.S. 128, 136 (1978) (holding, in the context of Title III minimization, that there should be an "objective assessment of the [agents'] actions in light of the facts and circumstances confronting [them] at the time"). Courts have accordingly assessed compliance with FISA minimization requirements under a "rule of reason," *see, e.g.*, *Chi Ping Ho*, 2018 WL 5777025, at *7, with the understanding that "Congress did not intend for nominal failure to abide the minimization procedures to undercut entire investigations," *United States v. Aziz*, 228 F. Supp. 3d 363, 378 (M.D. Pa. 2017).

Moreover, FISA expressly provides that the government is not required to minimize information that is "evidence of a crime," even if it is not foreign intelligence information. 50 U.S.C. §§ 1801(h)(3), 1821(4)(c). As a result, to the extent that certain communications of a United States person may be evidence of a crime or otherwise may establish an element of a substantive or conspiratorial offense, such communications need not be minimized. *See, e.g.*, *Chi Ping Ho*, 2018 WL 5777025, at *6.

Even if certain communications were not minimized in accordance with the SMPs, suppression would not be the appropriate remedy with respect to those communications that met the standard. As discussed above, absent evidence that there has been a complete disregard for the minimization procedures, the fact that some communications should have been minimized does not affect the admissibility of others that were properly acquired and retained. FISA's legislative history indicates that Congress intended only a limited sanction for errors of minimization:

> As the language of the bill makes clear, only that evidence which was obtained unlawfully or derived from information obtained unlawfully would be suppressed. If, for example, some information should have been minimized but was not, only that information should be suppressed; the other information obtained lawfully should not be suppressed.

H.R. Rep. No. 95-1283, pt. 1, at 93; *see also Medunjanin*, 2012 WL 526428, at *12 (disclosure and suppression not warranted where "failure to adhere to [the minimization] protocol was *de minimis*"); *Liu*, 2021 WL 6127396, at *3 (similar); *Chi Ping Ho*, 2018 WL 5777025, at *7 ("Although the Government acknowledged that in 'limited occasions described herein, certain communications were not properly minimized,' the Court finds that the Government's failure . . . in these instances was *de minimis* and that on the whole the agents have shown a high regard for the right of privacy and have done all they reasonably could to avoid unnecessary intrusion" (internal quotation marks and citations omitted)).

2. The FISA Information Was Appropriately Minimized

[CLASSIFIED INFORMATION REDACTED]

Based upon this information, the Government lawfully conducted the FISA collection discussed herein, and this Court should find that the FISA collection was lawfully conducted under the minimization procedures approved by the FISC and applicable to the FISA collection.

V. THE COURT SHOULD REJECT TERRY'S LEGAL ARGUMENTS

Terry asks this Court to "scrutinize the FISA applications and materials, suppress any evidence and fruits that were obtained unlawfully, and order disclosure of the FISA materials to the defense." (Mem. 46). Terry correctly requests "that the Court review such materials *in camera* and *ex parte*" and concedes "that 'disclosure of the FISA materials [to the defense] is the exception and *ex parte*, *in camera* determination is the rule.' *Abu Jihaad*, 630 F.3d at 129." (*See* Mem. 48, 50). Through this brief and Classified Appendix, the Government agrees to and satisfies Terry's request for this Court's *in camera* and *ex parte* review of the FISA materials.

Such review, however, will reveal that neither suppression nor disclosure to Terry is justified, however, and thus this Court should deny Terry's additional requests for suppression and disclosure as without merit.

A. TERRY HAS NOT ESTABLISHED ANY BASIS TO SUPPRESS THE FISA INFORMATION

In support of her request to suppress the FISA information, Terry alleges that (1) the Government engaged in "extreme and unwarranted surveillance tactics" when it used FISA to collect her communications rather than using Title III authorities to obtain a traditional search warrant; (2) the FISA applications at issue contain false representations and omissions, rendering the FISC's probable cause determinations defective; and (3) the FISA applications at issue relied on Terry's First Amendment-protected activity, rendering the FISC's probable cause determinations defective. (*See* Mem. 48-50). While Terry alleges she was the target of the FISA applications at issue, the Government does not publicly identify the target of FISA applications, including the FISA applications at issue. This Court should reject each of these arguments for the reasons discussed below.

1. The FISA Application(s) and Certification(s) Satisfied the Applicable "Significant Purpose" Standard

Terry first contends that the FISA information should be suppressed because the Government improperly instituted FISA surveillance for a criminal investigation, rather than for gathering of foreign intelligence, and the Government should have sought a search warrant under Title III rather than applying for a FISA warrant. (*See* Mem. 48-49). Courts, including this Court, have consistently denied such speculative claims, *e.g.*, *Abu Jihaad*, 630 F.3d at 120[20]; this

[20] The court's analysis in *Abu-Jihaad* relied to a significant extent on the U.S. Supreme Court's decision in *Keith*. There, in considering the Fourth Amendment's warrant requirement and the standards for conducting traditional law enforcement wiretapping under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (hereinafter, "Title III"), the Court

Court should similarly deny this speculative claim in the instant matter.

[CLASSIFIED INFORMATION REDACTED]

As part of the USA PATRIOT Act, Congress amended FISA to require that an Executive Branch official now certify that "a significant purpose" of the requested surveillance was to obtain foreign intelligence information. 18 U.S.C. § 1804(a)(6)(B). The "significant purpose" standard has been repeatedly upheld by numerous courts, including the Second Circuit, which observed in *Abu-Jihaad*, "we identify no constitutional infirmity in Congress's decision to allow FISA warrants to issue on certification of a 'significant purpose' to obtain foreign intelligence information. . . ." 630 F.3d at 131; *see also id.* at 128 (concluding that the standard "is sufficient to ensure that the executive may only use FISA to obtain a warrant when it is in good faith pursuing foreign intelligence gathering. . . ."); *Duka*, 671 F.3d at 343 ("the dispositive issue is whether the 'significant purpose' test is reasonable. . . . We agree with our sister courts of appeals and the Foreign Intelligence Surveillance Court of Review that the amended FISA's 'significant purpose' standard is reasonable under the Fourth Amendment.").

[CLASSIFIED INFORMATION REDACTED]

In sum, this Court's *in camera*, *ex parte* review of the FISA materials will dispel any impression that the certification(s) were somehow flawed. To the contrary, the required certification(s) and statements were properly made and were included in the application(s) at issue, the foreign intelligence interests of the United States were a significant purpose of the electronic surveillance and physical search, and the application(s) sought the type of foreign intelligence information identified. For these same reasons, and considering that the

---

indicated that the Fourth Amendment would countenance different standards for a warrant to conduct domestic security surveillance. *See id.* at 321–22.

certification(s) are presumed to be valid, this Court should deny Terry's suppression motion.

2. *Franks v. Delaware* Does Not Require Suppression of the FISA Information or Disclosure of the FISA Materials

Terry next argues that the FISA information should be suppressed because the FISA applications contain "false representations and omissions, rendering the FISC's probable cause determinations defective." (*See* Mem. 49-50). Specifically, based on its presence in a search warrant affidavit and the Indictment, Terry speculates that the FISA application(s) also included a purportedly false report that Terry was being paid by the ROK Government to write a particular magazine article.[21] (Mem. 49-50). Terry does not move this Court to conduct a *Franks* hearing; instead, in a footnote, she merely states that she would "welcome such a hearing if helpful to the Court." (Mem. 49, n. 47). As the Court's review of the FISA materials will show, no material false statements or omissions exist regarding the FISA information. Thus, this Court should deny Terry's suppression motion and decline to hold a *Franks* hearing.

To merit a *Franks* hearing, a defendant must make a "substantial preliminary showing" that the affiant deliberately or recklessly included false statements, or failed to include material information, in the affidavit, and that the resulting misrepresentation was essential to the finding of probable cause. *Franks*, 438 U.S. at 155–56. Courts apply the same standard when a defendant seeks a *Franks* hearing as part of a challenge to FISA collection: to obtain a hearing, a defendant must "make 'a substantial preliminary showing that a false statement knowingly or intentionally, or with reckless disregard for the truth, was included' in the application and that the allegedly false statement was 'necessary' to the FISA Judge's approval of the application."

[21] Terry also alleges that the FISA applications omitted necessary context regarding her journalistic work, and that the Government relied on "protected conduct" in its applications to the FISC. (*See* Mem. 49). The Government addresses this argument in Section V.A.3., below.

Duggan, 743 F.2d at 77 n.6 (quoting *Franks*, 438 U.S. at 155-56). Only after a defendant makes the requisite showing may the Court conduct a *Franks* hearing to determine if there are material misrepresentations of fact, or omissions of material fact, in the FISA applications sufficient to warrant suppression of the FISA-obtained or -derived evidence.[22] *See Franks*, 438 U.S. at 171.

While many courts have acknowledged the difficulty for defendants to meet this burden in cases in which information obtained or derived from FISA is being used against them, they agree that the *Franks* evidentiary burden still must be met. *See Daoud*, 755 F.3d at 483-84 ("Defense counsel would like to mount [a *Franks*] challenge in this case. But that's hard to do without access to the classified materials. . . . The drafters [of FISA] devised a solution: the judge makes the additional determination, based on full access to all classified materials and defense's proffer of its version of events, of whether it's possible to determine the validity of the *Franks* challenge without disclosure of any of the classified materials to the defense."); *Belfield*, 692 F.2d at 148 ("Congress was also aware of these difficulties [faced by defense counsel without access to FISA materials and] chose to resolve them through means other than mandatory disclosure."); *see also United States v. Alwan*, No. 1:11-CR-13-R, 2012 WL 399154, at *8-10 (W.D. Ky. Feb. 7, 2012) ("The Court is cognizant of the substantial difficulties [the defendant] has encountered in trying to assert a *Franks* violation. Regardless of the difficulties, however, it does not change the evidentiary burdens he must meet.").

[CLASSIFIED INFORMATION REDACTED]

---

[22] Indeed, even if a defendant offers sufficient proof to show that an affidavit involved false statements or omissions, a hearing should not be held where the affidavit would still provide probable cause if the allegedly false material were eliminated, or if the allegedly omitted information were included. *Franks*, 438 U.S. at 171; *United States v. Colkley,* 899 F.2d 297, 300 (4th Cir. 1990); *United States v. Ketzeback*, 358 F.3d 987, 990 (8th Cir. 2004); *United States v. Martin*, 615 F.2d 318, 328 (5th Cir. 1980).

Moreover, this Court should decline Terry's request—to the extent she makes one—to hold a *Franks* hearing. Again, Terry did not actually request a *Franks* hearing: she merely "would welcome such a hearing if helpful to the Court." (Mem. 49, n. 47). She also did not make the required "substantial preliminary showing." Accordingly, Terry failed to carry her burden of establishing the prerequisites for an adversarial hearing, and any attempt to obtain disclosure of the FISA materials to meet that burden runs counter to FISA, *Franks*, precedent, and Congressional intent. This Court's *in camera*, *ex parte* review of the FISA materials will demonstrate that "an adversary hearing in this case would be academic because there is no question the FISA applications pass muster." *Medunjanin*, 2012 WL 526428, at *9. Given that Terry has not met (or attempted to meet) the required standard, it would be improper for this Court to conduct a *sua sponte Franks* hearing.

3. The FISA Application(s) Was/Were Not Based Solely on First Amendment-Protected Activities

Terry next alleges that the FISC's probable cause determinations were defective because the government relied on her "protected [First Amendment activities] in its applications to the FISC" and "omitted necessary context that would have made apparent to the FISC that these activities amounted to [First Amendment protected] conduct." (Mem. 49). In doing so, Terry misstates the law, omitting the word "solely" from 50 U.S.C. § 1805(a)(2)'s requirement that "no United States person may be considered a foreign power or an agency of a foreign power *solely* upon the basis of activities protected by the first amendment to the Constitution of the United States . . . ." (emphasis added).[23] As discussed below, and as this Court's *ex parte*, *in camera* review will confirm, the FISA application(s) established ample probable cause, apart from any

[23] The Government notes that Terry cited the correct standard, including the critical "solely" modifier, two pages earlier in her motion. (Mem. 47).

First Amendment-protected activities, and the FISC's probable cause determination did not *solely* rely on First Amendment-protected activities.

As discussed in Section II.C, the FISC may consider First Amendment-protected activities if they are not the sole basis for finding that the target is an agent of a foreign power. *See* 50 U.S.C. §§ 1805(a)(2)(A) and 1824(a)(2)(A); *Rosen*, 447 F. Supp. 2d at 549-50; *Rahman*, 861 F. Supp. at 252. As the *Rosen* court noted, from FISA's "plain language, it follows that the probable cause determination may rely in part on activities protected by the First Amendment, provided the determination also relies on activities not protected by the First Amendment." 477 F. Supp. 2d at 548. And of course, the First Amendment does not protect all speech or advocacy-related activities. "Numerous crimes under the federal criminal code are, or can be, committed by speech alone. . . . [I]f the evidence shows that the speech[] crossed the line into criminal solicitation, procurement of criminal activity, or conspiracy to violate the laws, the prosecution is permissible." *Rahman*, 189 F.3d at 117.

[CLASSIFIED INFORMATION REDACTED]

B. TERRY HAS NOT ESTABLISHED ANY BASIS FOR DISCLOSING THE FISA MATERIALS

1. Disclosure is Not "Necessary" under FISA Section 1806(f)

Terry seeks disclosure of the FISA materials under 50 U.S.C. § 1806(f) if this Court identifies irregularities during its *in camera, ex parte* review. (Mem. 50). However, the presence of "irregularities" is not the appropriate legal standard for the compelled disclosure of FISA materials, as courts may only disclose the FISA materials when "such disclosure is *necessary* to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f) (emphasis added). Thus, there is only one lawful reason to disclose the FISA materials to defense counsel: that after its review of those materials *in camera* and *ex parte*, this Court

cannot determine the legality of the electronic surveillance, physical search, or both, without defense counsel's assistance. 50 U.S.C. §§ 1806(f), 1825(g); *Daoud*, 755 F.3d at 482; *Duggan*, 743 F.2d at 78. This holding is supported by the legislative history of 50 U.S.C. § 1806(f), which states: "The court may order disclos[ure] to [the defense] . . . only if it finds that such disclosure is necessary to make an accurate determination of the legality of the surveillance . . . Once a judicial determination is made that the surveillance was lawful, a motion for discovery . . . must be denied unless disclosure or discovery is required by due process." S. Rep. No. 95-701, at 64-65, 1978 U.S.C.C.A.N., at 4034; *see also United States v. Hassan*, 742 F.3d 104, 138 (4th Cir. 2014) (where the court "emphasized that, where the documents 'submitted by the government [are] sufficient' to 'determine the legality of the surveillance,' the FISA materials should not be disclosed") (quoting *Squillacote*, 221 F.3d at 454).

Here, Terry makes no attempt to establish that this Court cannot determine the legality of the FISA collection without defense counsel's assistance. She flags no issues where counsel's input would be "necessary," and fails to explain why this Court cannot address any issues like every other district court has done. As this Court will see from its review, the FISA materials contain no "irregularities," and are presented in a well-organized and straightforward manner that allows this Court to determine the lawfulness of the FISA collection without input from Terry's counsel.

Further, Terry is not entitled to the FISA materials to bolster her challenge to the lawfulness of the FISA authorities, as FISA's plain language precludes defense counsel from accessing the classified FISA materials to conduct a fishing expedition. In *Medunjanin*, the court noted that "[d]efense counsel . . . may not inspect the FISA dockets to construct a better argument for inspecting the FISA dockets. Such a circular exercise would be patently inconsistent with FISA . . . ." 2012 WL 526428, at *10. *See also Badia*, 827 F.2d at 1464 (rejecting the defendant's request for "disclosure of

the FISA application, ostensibly so that he may review it for errors"); *Mubayyid*, 521 F. Supp. 2d at 131 ("The balance struck under FISA . . . would be substantially undermined if criminal defendants were granted a right of disclosure simply to ensure against the possibility of a *Franks* violation.").

Terry fails to present any colorable basis for disclosure, as this Court can review and decide the legality of the FISA collection without defense counsel's assistance. Where, as here, defense participation is not necessary, FISA requires that the FISA materials remain protected from disclosure. Congress' clear intention is that FISA materials should be reviewed *in camera* and *ex parte* and in a manner consistent with the realities of modern intelligence needs and investigative techniques. There is nothing extraordinary about this case that would prompt this Court to order the disclosure of highly sensitive and classified FISA materials. *See Rosen*, 447 F. Supp. 2d at 546 (the "exceptional nature of disclosure of FISA material is especially appropriate in light of the possibility that such disclosure might compromise the ability of the United States to gather foreign intelligence information effectively") (citing *Belfield*, 692 F.2d at 147). Accordingly, even if this Court finds that Terry has properly moved for disclosure under 50 U.S.C. § 1806(f), it should deny her request for disclosure.

2. The FISA Dockets Do Not Present Any *Brady* or Due Process Concern That Would Merit Disclosure of the FISA Materials

Terry also invokes 50 U.S.C. § 1806(g) to request all FISA materials that are discoverable under *Brady v. Maryland*, 373 U.S. 83 (1963). (Mem. 50). The Government submits that this Court's review of the FISA materials will not reveal any material that due process requires be disclosed to Terry, such as *Brady* material, as provided for by 50 U.S.C. §§ 1806(g) and 1825(h). Accordingly, the provisions concerning due process in 50 U.S.C. §§ 1806(g) and 1825(h) cannot justify disclosure of, or an adversary hearing with respect to, the FISA materials at issue.

As noted above, FISA provides that once a district court has concluded that electronic surveillance and physical search were "lawfully authorized and conducted," "it shall deny the motion of the aggrieved person *except to the extent that due process requires discovery or disclosure*." 50 U.S.C. §§ 1806(g), 1825(h) (emphasis added). Courts agree that FISA's *in camera, ex parte* review does not violate the Due Process Clause of the Fifth Amendment, nor does due process require that defendant be granted access to the FISA materials, except as provided for in 50 U.S.C. §§ 1806(f), (g) and 1825(g), (h).[24] Moreover, Terry cannot identify any due process violation arising from the application of FISA's review procedures.

The plain intention of 50 U.S.C. §§ 1806(g) and 1825(h)—allowing this Court to order disclosure of material to which the defendant would be entitled under the Due Process Clause, such as material that had not been previously disclosed under *Brady*, even while ruling against the defendant's motion generally—cannot be interpreted to support Terry's demand for access to all of the FISA materials in advance of this Court's *in camera, ex parte* review and determination of the legality of the collection. The necessity of disclosing FISA materials is a factual, not a legal, question. With respect to any claim that the FISA materials contain information that due process requires be disclosed to the defense, the request is premature since this Court will make that factual determination for itself during its *in camera, ex parte* review. The Government submits that, for the reasons covered at length above, the Court's review will not identify any material due process or *Brady* concerns.

---

[24] *See, e.g.*, *Belfield*, 692 F.2d at 148-49; *El-Mezain*, 664 F.3d at 567; *Abu-Jihaad*, 630 F.3d at 129; *Damrah*, 412 F.3d at 624; *Ott*, 827 F.2d at 476-77; *Nicholson*, 955 F. Supp. at 592 (a judge in this district found, based on "the unanimous holdings of prior case law, . . . that FISA does not violate the Fifth or Sixth Amendments by authorizing *ex parte in camera* review"); *Benkahla*, 437 F. Supp. 2d at 554; *U.S. v. Jayyousi*, 2007 WL 851278 (S.D. Fla. Mar. 15, 2007) ; *Falvey*, 540 F. Supp. at 1315-16.

VI. CONCLUSION: THERE IS NO BASIS TO DISCLOSE THE FISA MATERIALS OR SUPPRESS THE FISA INFORMATION

Based on the analysis above, the Government submits that this Court must conduct an *in camera*, *ex parte* review of the FISA materials and the Government's classified submission. The Government further submits that, following such review, this Court should: (1) find that disclosure of the FISA materials and the Government's classified submissions to Terry is not authorized because the Court is able to make an accurate determination of the legality of the surveillance and searches without disclosure; (2) find that the electronic surveillance and physical search at issue were both lawfully authorized and conducted in compliance with FISA; (3) hold that the fruits of the electronic surveillance and physical search should not be suppressed; and (4) order that the FISA materials and the Government's classified submissions be maintained under seal by the Classified Information Security Officer or his or her designee.[25]

[25] A district court order granting motions or requests under 50 U.S.C. §§ 1806(g) or 1825(h), a decision that electronic surveillance or physical search was not lawfully authorized or conducted, and an order requiring the disclosure of FISA materials are each a final order for purposes of appeal. *See* 50 U.S.C. §§ 1806(h), 1825(i). Should the Court conclude that disclosure of any item within any of the FISA materials or suppression of any FISA-obtained or -derived information may be required, given the significant national security consequences that would result from such disclosure or suppression, the Government would expect to pursue an appeal. Accordingly, the Government respectfully requests the Court stay any such order pending an appeal by the United States of that order.

Dated: June 17, 2025

Respectfully Submitted,

JAY CLAYTON
United States Attorney

By: /s/
Kyle Wirshba
Samuel Adelsberg
Chelsea L. Scism
Assistant U.S. Attorneys
United States Attorney's Office
Southern District of New York

Christina Clark
Trial Attorney
National Security Division
U.S. Department of Justice

Exhibit A

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,	)	24 Cr. 427 (LGS)
v.	)	
SUE MI TERRY,	)	
Defendant.	)	

DECLARATION AND CLAIM OF PRIVILEGE OF THE ATTORNEY GENERAL

I, Pamela Bondi, hereby declare the following:

1. I am the Attorney General of the United States and the head of the U.S. Department of Justice. I have official custody of and control over the relevant files and records of the U.S. Department of Justice. The matters stated herein are based on my knowledge, on consideration of information available to me in my official capacity as the Attorney General, on discussions that I have had with other Department of Justice officials, and on conclusions I have reached after my review of this information.

2. Under the authority of 50 U.S.C. §§ 1806(f) and 1825(g), I submit this declaration pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended, in connection with the above-captioned criminal proceeding. I have been advised that the Government presently intends to use information obtained or derived from FISA-authorized electronic surveillance and physical search in the criminal proceedings against the Defendant, Sue Mi Terry. *See* 50 U.S.C. §§ 1806(c), 1825(d). I understand that the Defendant was provided notice of the Government's intent to use FISA information and that the Defendant, by and through her attorney, has filed a motion seeking suppression of all evidence obtained or derived under FISA, and disclosure of the application(s) submitted to, and the order(s) issued by, the Foreign

Intelligence Surveillance Court, and other related materials (collectively, the "FISA Materials"). The Government is opposing the Defendant's Motion. For the reasons set forth in the Government's opposition, it is necessary to provide this Court with the FISA Materials.

3. Based on the facts and considerations set forth below, I hereby claim that it would harm the national security of the United States to disclose or hold an adversary hearing with respect to the FISA Materials. *See* 50 U.S.C. §§ 1806(f), 1825(g). The United States will be submitting the relevant classified documents to this Court as part of a Sealed Appendix, so that this Court may conduct an *in camera, ex parte* review of the FISA Materials. My Claim of Privilege also extends to the classified portions of any memoranda, briefs, or other documents the Government may file in connection with this litigation and to any oral representations that may be made by the Government that reference the classified information contained in the FISA Materials.

4. In support of my Claim of Privilege, the United States is submitting to the Court for *in camera, ex parte* review the Declaration of Roman Rozhavsky, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation. The Declaration of Assistant Director Rozhavsky sets forth in detail the specific facts on which my Claim of Privilege is based. The Declaration of Assistant Director Rozhavsky is classified at the "TOP SECRET" level. The FISA Materials are classified at the "TOP SECRET" and "SECRET" levels.

5. Relying on the facts set forth in the Declaration of Assistant Director Rozhavsky, I certify that the unauthorized disclosure of the FISA Materials that are classified at the "TOP SECRET" level could reasonably be expected to cause exceptionally grave damage to the national security of the United States. I further certify that the unauthorized disclosure of the FISA Materials that are classified at the "SECRET" level could reasonably be expected to cause serious damage to the national security of the United States. The FISA Materials contain

sensitive and classified information concerning United States intelligence sources and methods and other information related to efforts of the United States to conduct counterintelligence investigations, including the manner and means by which those investigations are conducted. As a result, the unauthorized disclosure of the information could harm the national security interests of the United States.

6. I respectfully request that the Court treat the contents of the Sealed Appendix, for security purposes, in the same sensitive manner that the contents were treated in the submission to this Court, and to return the Sealed Appendix to the Department of Justice upon the disposition of the Defendant's Motion. The Department of Justice will retain the Sealed Appendix under the seal of the Court subject to any further orders of this Court or other courts of competent jurisdiction.

Pursuant to Title 28, United States Code, Section 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed on this 10 day of June, 2025.

Pamela Bondi
Attorney General